UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

IN RE ASHLEY MADISON CUSTOMER DATA SECURITY BREACH LITIGATION	)	
	)	**MDL No. 2669**
This Document Relates to:	)	
	)	**Case No. 4:15MD2669 JAR**
ALL CASES	)	

CONSOLIDATED CLASS ACTION COMPLAINT

COME NOW Plaintiffs Brian Farr, Steven Coward, Marc Benefield, Nhung Truong, Gustavo Alfaro, David Yagel, John Hiles III, Matthew Lisuzzo, Britt Garrett, Christopher Russell, David Miller, James Mike Shows, Todd Witengier, Byron Goetting, Marvin Cabiness, Keith Macomber, Paul Jack and Anthony Imbarrato, on behalf of themselves and all others similarly situated, and for their Consolidated Class Action Complaint state as follows:

NATURE OF THE ACTION

1. AshleyMadison.com describes itself as "the most famous name in infidelity and married dating" and as a website for "discreet encounters between married individuals." Plaintiffs bring this class action as a result of a breach of the security system of Defendants' AshleyMadison.com website, resulting in compromised security of Plaintiffs' and Class Members' highly confidential financial and personal information. Upon information and belief such information included, but was not limited to, highly sensitive information concerning the putative Class Members' (hereafter "Class Members") names, addresses, telephone numbers, credit or debit card numbers, email addresses, dates of birth, date of creation of accounts, last account update, account type, nickname, gender, ethnicity, sexual preferences, and relationship status ("Personal Information").

2. Plaintiffs also bring this class action because Defendants and others were engaged in a wire fraud conspiracy to employ the "Ashley Madison" website, which Defendants controlled, to carry out illegal and fraudulent conduct to the injury of Plaintiffs and the Class.

3. On some time prior to July 19, 2015, Defendants' databases were compromised, with the result that Plaintiffs and Class Members' Personal Information was used or is at risk of use in fraudulent transactions or identity theft around the world, as well as for invidious exposure, extortion, blackmail, and other illicit purposes. Upon information and belief, Defendants maintain or maintained information, including Personal Information, regarding nearly 37 million subscribers, and Defendants' security failures affected the Personal Information of hundreds of thousands if not millions of customers, including Plaintiffs and the Class Members.

4. Defendants made numerous deceptive and misleading statements regarding the safety and security of their Ashley Madison website in an effort to induce the public to submit their highly confidential Personal Information to the website. Among other things, beginning in approximately 2011, Defendants contended that the Defendants and/or the Ashley Madison website had been awarded a "Trusted Security Award" which, according to published reports, does not exist.

5. Upon information and belief, the security breach and theft of Personal Information was caused by Defendants' violations of their obligations to abide by the best practices and industry standards concerning data security, as well as applicable federal law and regulations.

6. After learning of the security breach, Defendants failed to notify Plaintiff and the Class Members in a timely manner and failed to take other reasonable steps to inform them of

the nature and extent of the breach. As a result, Defendants prevented Plaintiffs and the Class Members from protecting themselves from the breach and caused Plaintiffs and Class Members to suffer financial loss and other substantial losses as described herein.

7. Furthermore, the security breach disclosed that Defendants had engaged in a campaign to deceive and defraud their customers. Among other things, Defendants had promised that, in return for payment, Defendants offered a "full delete" or "paid delete" option which would delete highly confidential Personal Information in Defendants' possession. Defendants represented that this option would "remove all traces of your usage[.]"

8. Defendants accepted payments for the "paid delete" option from Plaintiffs and the Class Members, but did not delete all of the Personal Information promised, a fact made clear when the data breach exposed the identifying Personal Information of Plaintiffs who had purchased the "paid delete" option. For example, some Plaintiffs and Class Members purchased the "paid delete" option prior to the security breach but nevertheless received extortion threats that included Personal Information which could not have been obtained except through the breach.

9. Furthermore, on information and belief, many of the website's claimed 38 million "members" were actually fake profiles or "bot" accounts created and maintained by Defendants. As set forth more fully below, Defendants employed these "bots" to mislead and deceive the Class into believing that payments were being made to interact with other members of the site, when in fact members were paying to interact with computer programs. The use of these fraudulent bots was instrumental in driving income to the website.

10. Defendants have benefitted from extracting money from Plaintiffs and the Class Members under false pretenses. Plaintiffs have been harmed by those payments for worthless

services and by the public disclosure of their highly sensitive financial and personal information. Indeed, for many of the website's members, the fact that this information has been made public has caused and will continue to cause irreparable harm, including public humiliation, ridicule, divorce, extortion, loss of employment, and increased substantial risk of identity theft and other types of fraud, among other catastrophic personal and professional harm.

11. Many of the Plaintiffs herein and numerous Class Members have received emails and other communications attempting to extort or blackmail them as a result of the data breach, based on their use of the Ashley Madison website. These extortion attempts include Personal Information obtained through the data breach. Nevertheless, Defendants have done little to remedy the harm they have caused.

12. Plaintiffs, on behalf of themselves and all others similarly situated, assert the following claims on behalf of a nationwide class: Violation of the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. §1962 (Count I) and Violation of the Stored Communications Act ("SCA") 18 U.S.C. § 2702 (Count II).

13. Plaintiffs further assert the following claims on behalf of a nationwide class, or in the alternative, statewide subclasses for the states of Alabama, Arizona, Arkansas, California, Colorado, Florida, Illinois, Louisiana, Maryland, Minnesota, Mississippi, Missouri, Nevada, New Jersey, North Carolina, Virginia and Washington: Negligence and negligence per se (Count III); breach of implied contract (Count IV); breach of contract (Count V); unjust enrichment (Count VI); and negligent misrepresentation (Count VII).

14. Plaintiffs, on behalf of themselves and all others similarly situated, also assert claims on behalf of statewide classes for the violation of state consumer fraud statutes, as set forth in Count VIII, including, without limitation: The Alabama Deceptive Trade Practices Act,

Ala. Code §§ 8-19-1 *et seq.*; Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1521, *et seq.*; Arkansas Deceptive Trade Practices Act, Ark. Code Ann. § 4-88-101 *et seq.*; California Consumers Legal Remedies Act, California Civil Code §1750, *et seq.*; California Unfair Competition Law, California Business and Professions Code §17200, *et seq.*; and California False and Misleading Advertising Law, California Business and Professions Code §17500, *et seq.*; Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-101, *et seq.*; Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*; Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*; Louisiana Unfair Trade Practices and Consumer Protection Act, La. Rev. Stat. Ann. § 51:1405 *et seq.*; Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-101 *et seq.*; Minnesota Consumer Fraud Act, Minn. Stat. §§325F.68-325F.69 *et seq.*; Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1, *et seq.*; Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 41.600 *et seq.* and Nev. Rev. Stat. §§ 598.0915-598.0925; New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56-8-19, *et seq.*; North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1 *et seq.* Virginia Consumer Protection Act, Va. Code § 59.1-196 *et seq.*; Washington Consumer Protection Act, Rev. Code Wash. Ann. § 19.86.010, *et seq.*, and the substantially similar consumer protection statutes of other states in which Defendants transact business.

15. Plaintiffs Nhung Truong and Gustavo Alfaro, on behalf of themselves and all others similarly situated, assert Count IX for violations of the California Customer Records Act on behalf of a class of California consumers.

16. Plaintiffs, on behalf of themselves and all others similarly situated, also assert claims on behalf of statewide classes for the violation of state data breach notice statutes, as set forth in Count X, including: Ariz. Rev. Stat. § 44-7501; Ark. Code § 4-110-101 *et seq.*; Cal. Civ.

Code §§ 1798.29, 1798.80 *et seq.*; Colo. Rev. Stat. § 6-1-716;; 815 ILCS §§ 530/1 to 530/25; Fla. Stat.§§ 501.171, 282.0041, 282.318(2)(i); La. Rev. Stat. §§ 51:3071 *et seq.*, 40:1300.111 to .116; Md. Code Com. Law §§ 14-3501 *et seq.*, Md. State Govt. Code §§ 10-1301 to -1308; Minn. Stat. §§ 325E.61, 325E.64; Miss. Code § 75-24-29; Mo. Rev. Stat. § 407.1500; N.J. Stat. § 56:8-161, 163; N.C. Gen. Stat §§ 75-61, 75-65; Va. Code § 18.2-186.6, § 32.1-127.1:05, § 22.1-20.2; and Wash. Rev. Code § 19.255.010, 42.56.590, 2015 H.B. 1078, Chapter 65, and the substantially similar data breach notice statutes of other states in which Defendants transact business.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, which confers upon the Court original jurisdiction over all civil actions arising under the laws of the United States, and pursuant to 18 U.S.C. § 2707 and 18 U.S.C. § 1964. This Court has supplemental jurisdiction over Plaintiffs' and Class Members' state law claims under 28 U.S.C. § 1367.

18. In addition, this Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action with more than 100 members and where the aggregate claims of all Class Members are in excess of $5,000,000.00, exclusive of interest and costs, and the Class Members do not share citizenship with Defendants. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d) because the matter in controversy exceeds $75,000.00, exclusive of interest and costs, and Defendants are citizens and subjects of a foreign state.

19. This Court has personal jurisdiction over Defendants because Defendants:

a. intentionally and purposefully availed themselves of this jurisdiction by marketing their website to millions of consumers, including residents throughout Missouri and this District;

b. have directed tortious acts toward individuals residing within this District, and have committed tortious acts that they know or should have known would cause injury to the Plaintiffs and Class Members in this District;

c. have committed overt acts in support of their conspiracy in violation of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §1962, within this District, including wire fraud by directing fraudulent electronic messages through the internet to Plaintiffs and Class Members in this District; and

d. have transacted substantial business in this state, including entering into contracts with thousands of Missouri Residents, including Plaintiff Witengier and other residents of this District, and because said business and contracts form part of the subject matter of this suit.

20. Each of the Defendants have engaged in conduct intentionally designed to solicit business from consumers in the State of Missouri and in this District. This includes the fraudulent and tortious communications directed through the Ashley Madison website to users located in the State of Missouri, as described herein, which Defendants knew were directed to Missouri residents, as Defendants were in possession of Plaintiffs' and the Class Members' addresses. Furthermore, Defendants ran advertisements designed to solicit business for the Ashley Madison website from consumers in the State of Missouri and in this District.

21. Venue is properly set in this District pursuant to 28 U.S.C. § 1391(b) since Defendants transact business within this judicial district. Likewise, a substantial part of the

events giving rise to the claim occurred within this judicial district.

PARTIES

22. At all relevant times, Plaintiff Brian Farr was a citizen and resident of the State of Alabama. Plaintiff Farr accessed the Ashley Madison website and created an account in approximately 2011. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his name and email address. Plaintiff purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code. Prior to the data breach, in 2012 and in 2014, Plaintiff purchased the "paid delete" option from Defendants in reliance on the promise that the option would remove all traces of usage.

23. Plaintiff Farr was injured in that his confidential Personal Information was released on the internet in the data breach. Plaintiff was injured in paying for a "paid delete" option, which did not remove all traces of his usage of the website but instead was exposed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users, Plaintiff would not have created a profile and/or would not have purchased the "paid delete" option.

24. Furthermore, on information and belief, at the time Plaintiff Farr first accessed the website there were no posted terms and conditions concerning arbitration or the waiver of any right to pursue claims against Defendants in class action proceedings, Plaintiff was never notified regarding any change in the terms and conditions of the website, and Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against

Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such arbitration provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

25. At all relevant times, Plaintiff Steven Coward was a citizen and resident of the State of Arizona. Plaintiff Coward accessed the Ashley Madison website and created an account in approximately 2010. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff Coward purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

26. Plaintiff Coward was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased credits on the site.

27. Furthermore, on information and belief, at the time Plaintiff Coward first accessed the website there were no posted terms and conditions concerning arbitration or the waiver of any right to pursue claims against Defendants in class action proceedings, Plaintiff was never notified regarding any change in the terms and conditions of the website, and Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

28. At all relevant times, Plaintiff Marc Benefield was a citizen and resident of the State of Arkansas. Plaintiff Benefield accessed the Ashley Madison website and created an account in April of 2015. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his name and email address. Plaintiff purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

29. Plaintiff was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he

purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased credits on the site.

30. Furthermore, on information and belief, Plaintiff Benefield has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such arbitration provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

31. At all relevant times, Plaintiff Nhung Truong was a citizen and resident of the State of California. Plaintiff Truong accessed the Ashley Madison website and created an account in approximately May of 2008, and terminated her account in January of 2010. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including photographs, her address, and her email address. Prior to the data breach, Plaintiff purchased the "paid delete" option from Defendants in reliance on the promise that the option would remove all traces of usage. In order to purchase

the "paid delete" option, Plaintiff was required to provide her full name, street address, and her credit and/or debit card number and CVV code.

32. Nevertheless, Plaintiff Truong was injured in that her confidential Personal Information was released on the internet in the data breach. Furthermore, Plaintiff was injured in paying for a "paid delete" option which did not remove all traces of her usage of the website, which was exposed in the data breach. Plaintiff has also received blackmail/extortion email threats as a direct result of the Ashley Madison data breach, which contained Personal Information which was disclosed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants did not intend to in fact remove all traces of her usage of the site, Plaintiff would not have created a profile and/or would not have purchased the "paid delete" option on the site.

33. Furthermore, on information and belief, at the time Plaintiff Truong first accessed the website there were no posted terms and conditions concerning arbitration or the waiver of any right to pursue claims against Defendants in class action proceedings, Plaintiff was never notified regarding any change in the terms and conditions of the website, and Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish her right to pursue his claims against Defendants in class action proceedings. Furthermore, on information and belief, Plaintiff ceased use of the website prior to the time that the terms and conditions contained references to arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that she was required to read and assent to before creating an account or using Defendants' website and messaging services, and

Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such arbitration provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

34. At all relevant times, Plaintiff Gustavo Alfaro was a citizen and resident of the State of California. Plaintiff Alfaro accessed the Ashley Madison website and created an account in approximately January of 2013. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. Prior to the data breach, Plaintiff also purchased the "paid delete" option from Defendants in reliance on the promise that the option would remove all traces of usage. In order to purchase credits and the "paid delete" option, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

35. Plaintiff was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Additionally, Plaintiff was injured in paying for a "paid delete" option which did not remove all traces of his usage of the website, which was exposed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users, that Defendants

employed fraudulent "bot" profiles, and that Defendants did not intend to in fact remove all traces of his usage of the site, Plaintiff would not have created a profile, would not have purchased credits on the site, and/or would not have paid for the "paid delete" option.

36. Furthermore, on information and belief, Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such arbitration provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

37. At all relevant times, Plaintiff David Yagel was a citizen and resident of the State of Colorado. Plaintiff Yagel accessed the Ashley Madison website and created an account for the first time in 2006. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff Yagel believes that he purchased at least $850 in credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

38. Plaintiff was injured in that his confidential Personal Information was released on the internet in the data breach. On information and belief, Plaintiff was injured in that he

purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Plaintiff has also received blackmail/extortion email threats as a direct result of the Ashley Madison data breach, containing Personal Information which was disclosed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased credits on the site.

39. Furthermore, on information and belief, at the time Plaintiff Yagel first accessed the website there were no posted terms and conditions concerning arbitration or the waiver of any right to pursue claims against Defendants in class action proceedings, Plaintiff was never notified regarding any change in the terms and conditions of the website, and Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

40. At all relevant times, Plaintiff John Hiles III was a citizen and resident of the State of Florida. Plaintiff Hiles accessed the Ashley Madison website and created an account in

approximately November of 2014. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his name and email address. Plaintiff purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code. Prior to the data breach, in December of 2014, Plaintiff purchased the "paid delete" option from Defendants in reliance on the promise that the option would remove all traces of usage.

41. Plaintiff was injured in that his confidential Personal Information was released on the internet in the data breach. Plaintiff was injured in paying for a "paid delete" option which did not remove all traces of his usage of the website, which was instead exposed in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Plaintiff has also received blackmail/extortion email threats as a direct result of the Ashley Madison data breach, containing Personal Information which was disclosed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased the "paid delete" option.

42. Furthermore, on information and belief, Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and

conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such arbitration provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

43. At all relevant times, Plaintiff Matthew Lisuzzo was a citizen and resident of the State of Illinois. Plaintiff Lisuzzo joined the website in 2008. Plaintiff created a profile on the site and provided confidential Personal Information, in reliance on Defendants' promise of absolute discretion, including his street address and email address. Plaintiff Lisuzzo also purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

44. Plaintiff Lisuzzo was injured in that his confidential Personal Information was released on the internet in the data breach, which resulted in the theft of his identity and money from his bank account. Plaintiff suffered financial and other losses in his attempts to remedy the situation, which remains unresolved. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information

of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased and spent credits on the site.

45. Furthermore, on information and belief, at the time Plaintiff Lisuzzo first accessed the website there were no posted terms and conditions concerning arbitration or the waiver of any right to pursue claims against Defendants in class action proceedings, Plaintiff was never notified regarding any change in the terms and conditions of the website, and Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

46. At all relevant times, Plaintiff Britt Garrett was a citizen and resident of the State of Louisiana. Plaintiff Garrett accessed the Ashley Madison website and created an account in approximately May of 2013. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff purchased approximately $650 in credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

47. Plaintiff Garrett was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Plaintiff has also received blackmail/extortion email threats as a direct result of the Ashley Madison data breach, containing Personal Information which was disclosed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased and spent credits on the site.

48. Furthermore, on information and belief, Plaintiff Garrett has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such arbitration provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

49. At all relevant times, Plaintiff Christopher Russell was a citizen and resident of the State of Maryland. Plaintiff Russell joined the Ashley Madison website in approximately March of 2011. Plaintiff created a profile on the site and provided confidential Personal

Information in reliance on Defendants' promise of absolute discretion, including his email address. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code. Plaintiff Russell purchased approximately $100 in credits for the purpose of sending messages to the profiles of other purported Ashley Madison users.

50. Plaintiff Russell was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Based on information now available, Plaintiff now believes that dozens of profiles he messaged on the site were in fact "bots." Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased and spent credits on the site.

51. Furthermore, on information and belief, at the time Plaintiff Russell first accessed the website there were no posted terms and conditions concerning arbitration or the waiver of any right to pursue claims against Defendants in class action proceedings, Plaintiff was never notified regarding any change in the terms and conditions of the website, and Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and

messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

52. At all relevant times, Plaintiff David Miller was a citizen and resident of the State of Minnesota. Plaintiff Miller accessed the Ashley Madison website and created an account in January of 2015. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

53. Plaintiff Miller was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Plaintiff has also received blackmail/extortion email threats as a direct result of the Ashley Madison data breach, containing Personal Information which was disclosed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased and spent credits on the site.

54. Furthermore, on information and belief, Plaintiff Miller has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such arbitration provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

55. At all relevant times, Plaintiff James Mike Shows was a citizen and resident of the State of Mississippi. Plaintiff Shows accessed the Ashley Madison website and created an account in approximately 2008 or 2009. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, such as biographical information, name, address, credit card information, and email address. Plaintiff Shows purchased approximately $600 in credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

56. Plaintiff Shows was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual

users of the website. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased credits on the site.

57. Furthermore, on information and belief, at the time Plaintiff Shows first accessed the website there were no posted terms and conditions concerning arbitration or the waiver of any right to pursue claims against Defendants in class action proceedings, Plaintiff was never notified regarding any change in the terms and conditions of the website, and Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

58. At all relevant times, Plaintiff Todd Witengier was a citizen and resident of the State of Missouri. Plaintiff Witengier accessed the Ashley Madison website and created an account in early 2013. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

59. Plaintiff Witengier was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was

injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Plaintiff has also received blackmail/extortion email threats as a direct result of the Ashley Madison data breach, containing Personal Information which was disclosed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased and spent credits on the site.

60. Furthermore, on information and belief, Plaintiff Witengier has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such arbitration provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

61. At all relevant times, Plaintiff Byron Goetting was a citizen and resident of the State of Nevada. Plaintiff Goetting accessed the Ashley Madison website and created an account in 2013. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff purchased credits for the purpose of sending messages to the profiles of other purported Ashley

Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

62. Plaintiff Goetting was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Plaintiff has also received blackmail/extortion email threats as a direct result of the Ashley Madison data breach, containing Personal Information which was disclosed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased and spent credits on the site.

63. Furthermore, on information and belief, Plaintiff Goetting has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such arbitration provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

64. At all relevant times, Plaintiff Marvin Cabiness was a citizen and resident of the State of New Jersey. Plaintiff Cabiness accessed the Ashley Madison website and created an account in approximately May of 2007. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff Cabiness purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

65. Plaintiff Cabiness was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Plaintiff has also received blackmail/extortion email threats as a direct result of the Ashley Madison data breach, containing Personal Information which was disclosed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased credits on the site.

66. Furthermore, on information and belief, at the time Plaintiff Cabiness first accessed the website there were no posted terms and conditions concerning arbitration or the waiver of any right to pursue claims against Defendants in class action proceedings, Plaintiff was never notified regarding any change in the terms and conditions of the website, and Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his

claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

67. At all relevant times, Plaintiff Paul Jack was a citizen and resident of the State of North Carolina. Plaintiff Jack accessed the Ashley Madison website and created an account in approximately early 2013. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff Jack purchased approximately $1500 in credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

68. Plaintiff Jack was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Plaintiff has also received blackmail/extortion email threats as a direct result of the Ashley Madison data breach, which contained Personal Information which was disclosed in the data breach. Had Plaintiff been aware of Defendants' misrepresentations

described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff Jack would not have created a profile and/or would not have purchased credits on the site.

69. Furthermore, on information and belief, Plaintiff Jack has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

70. At all relevant times, Plaintiff Keith Macomber was a citizen and resident of the State of Virginia. Plaintiff Macomber accessed the Ashley Madison website and created an account in May of 2008. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff Macomber purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

71. Plaintiff Macomber was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased credits on the site.

72. Furthermore, on information and belief, at the time Plaintiff Macomber first accessed the website there were no posted terms and conditions concerning arbitration or the waiver of any right to pursue claims against Defendants in class action proceedings, Plaintiff was never notified regarding any change in the terms and conditions of the website, and Plaintiff has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against Defendants in class action proceedings was formed and/or any such provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

73. At all relevant times, Plaintiff Anthony Imbarrato was a citizen and resident of the State of Washington. Plaintiff accessed the Ashley Madison website and created an account in

2013. Plaintiff created a profile on the site and provided confidential Personal Information in reliance on Defendants' promise of absolute discretion, including his email address. Plaintiff purchased credits for the purpose of sending messages to the profiles of other purported Ashley Madison users. In order to purchase credits, Plaintiff was required to provide his full name, street address, and his credit and/or debit card number and CVV code.

74. Plaintiff Imbarrato was injured in that his confidential Personal Information was released on the internet in the data breach. Further, on information and belief, Plaintiff was injured in that he purchased credits and/or paid to send messages as a result of Defendants' female profiles, which were in fact fraudulent "bots" created by Defendants, rather than actual users of the website. Plaintiff has also received blackmail/extortion email threats as a direct result of the Ashley Madison data breach, containing Personal Information which was disclosed in the data breach. Plaintiff also received a threatening letter at his home. Had Plaintiff been aware of Defendants' misrepresentations described herein, including that Ashley Madison does not adequately protect and secure the Personal Information of its users and that Defendants employed fraudulent "bot" profiles, Plaintiff would not have created a profile and/or would not have purchased and spent credits on the site.

75. Furthermore, on information and belief, Plaintiff Imbarrato has never agreed to arbitrate any dispute with Defendants or to relinquish his right to pursue his claims against Defendants in class action proceedings. On information and belief, Plaintiff was not presented with terms and conditions of service regarding arbitration and class waiver that he was required to read and assent to before creating an account or using Defendants' website and messaging services, and Plaintiff did not read or assent to any such terms and conditions of service. No valid contract regarding arbitration or the purported waiver of any right to pursue claims against

Defendants in class action proceedings was formed and/or any such arbitration provisions are substantively and procedurally unconscionable, conflict with other applicable laws, and are otherwise unenforceable against Plaintiff.

76. Defendant Avid Life Media, Inc. is a corporation organized under Canadian law with its headquarters and principal place of business in Toronto, Canada.

77. Defendant Avid Dating Life, Inc. is a corporation organized under Canadian law with its headquarters and principal place of business in Toronto, Canada.

78. Defendant Noel Biderman is a citizen and resident of Canada, and was formerly the Chief Executive Officer of Defendant Avid Life Media, Inc.

79. Doe Defendants #1 to #5 are managers, employees or agents of Defendants Avid Life Media, Inc., Avid Dating Life, Inc., and/or Noel Biderman, currently unknown to Plaintiffs, who controlled and managed the "Ashley Madison" dating website enterprise.

80. Unless otherwise specified, Defendants Avid Life Media, Inc., Avid Dating Life, Inc., Noel Biderman and Doe Defendants #1 to #5 are referred to collectively herein as "Defendants."

FACTUAL BACKGROUND COMMON TO ALL COUNTS

81. Defendants own, operate, and/or control social networking internet sites and services, including a site on the Internet branded as "Ashley Madison" and located at www.ashleymadison.com. The website was launched on or about January 21, 2002.

82. AshleyMadison.com is purportedly owned by Defendant Avid Life Media, a privately held Canadian corporation founded by Defendant Noel Biderman, its former Chief Executive Officer. Avid Life Media owns various companies that are in the business of

operating online dating websites. Defendant Avid Dating Life operates online dating websites, including AshleyMadison.com.

83. Defendants market AshleyMadison.com to consumers in the United States as well as to consumers in about 45 other countries. Defendants market Ashley Madison as a "discreet" website with over 38 million "anonymous members."

84. Defendants market the website through television, radio, billboard, and Internet advertisements throughout the United States of America, the State of Missouri, and this District.

85. Many of these advertisements featured Defendant Biderman as the website's spokesperson, personally encouraging the public to use Defendants' Ashley Madison website.

86. Due to the sensitive nature of the website and information a consumer was required to share to activate an account, Defendants marketed to consumers that its network system and the servers that contained consumers' Personal Information were carefully monitored and equipped with the highest levels of security and sophisticated data theft prevention systems that would ensure that users' Personal Information would not be obtained by third parties. Defendants intended for this marketing information to entice consumers into creating Ashley Madison accounts and utilizing the website.

87. On information and belief, Defendant Biderman has made numerous statements publicly and in the media asserting that the Ashley Madison website provided its users the highest possible security, above and beyond the level of security provided by other social media websites:

(a) "To us, the perfect affair is meeting someone and not being discovered, and so we have built a product that gears towards not being discovered . . . . The anonymous way you sign up, the discreet nature of our communications platform, the billing

being secretive, and ultimately, things like our ghost delete, which allows you to recall every message or photo that you have ever shared, and we even blow it off our own servers, which, by the way, sit in a remote location, kind of untouchable. So I think we do everything we can to protect privacy, way over and above what a service that is just catering to, say, a singles dating would ever do."

(b) "The perfect affair is not just meeting someone, it's not being discovered. So we really had to build the technology to help create the discretion. Unlike other websites you encounter, we're closed."

(c) "So the tools set up on AshleyMadison, the discrete nature of how we hide your photos, mask it, delete your profile, make it like a ghost, like you never existed are all features that help you have that perfect affair."

(d) "The object of a perfect affair is meeting someone and not getting discovered .... On a service where every step is looked at as how do we keep this private between you and this other person? How do we keep your photos under lock and key? How do we make it like you were a ghost like you were never here? How do we do all of those kind of things ... that's probably a service that would give you the best chance of not being discovered."

(e) "We have done a really great job of making sure our data is kept secret; the anonymity of it hopefully gives comfort to our members."

(f) "The technology I've built: the photo masquerading, the anonymous billing, even the way my messaging works-the password protection even to the Nth degree, where if you're on Ashley Madison and decide, hey, I want to eradicate my presence - I want to delete - you don't just delete (your profile) the way you would

> on Match.com or Facebook .... Only a service catering to discretion [] would ever build technology along those lines, and I think that's what makes us so fascinating."

88. Sometime prior to July 19, 2015, a team of hackers accessed databases owned, operated, or controlled by Defendants that process, store, or utilize information regarding Ashley Madison transactions and contain highly confidential Personal Information of Ashley Madison members. Upon information and belief, Defendants' data breach has impacted hundreds of thousands or millions of its customers within the United States. Defendants, although aware of the breach, did not initially disclose it to Ashley Madison members or the public.

89. On information and belief, on or about July 12, 2015 Defendants were notified by the hackers of the breach and that client information would be released unless the Ashley Madison website was taken down.

90. On or about July 19, 2015, the hackers publicly announced that they had gained access to the Ashley Madison database and threatened that they would publicly release the information if Defendants did not shut down the Ashley Madison website.

91. Defendants addressed the threat in a public statement the following day, July 20, 2015, falsely suggesting that the breach had been contained and that "our team has now successfully removed the posts related to this incident as well as all Personal Identifiable Information (PII) about our users published online."

92. On information and belief, by at least August 17, 2016, and after Defendants had refused or failed to take down the Ashley Madison website as demanded, the hackers released onto the internet the personal information of Ashley Madison's more than 30 million users,

including email addresses, physical addresses, certain credit card information and sexual preferences.

93. Prior to the data breach, Defendants promised, for a fee, to permanently delete the Personal Information of Ashley Madison users ("paid-delete") that would "remove all traces of your usage." In short, Defendants promised to erase all evidence of a member's usage on the website and all of their personally identifying information. On information and belief, numerous Ashley Madison users paid this fee and Defendants obtained millions of dollars in revenue from the "paid-delete" option.

94. Prior to the data breach, numerous Class Members, including Plaintiffs Nhung Truong, Gustavo Alfaro and John Hiles III, accepted Defendants' offer to "paid-delete" any Personal Information in Defendant's possession and paid Defendants for that service.

95. Defendants broke their promise to the Plaintiffs and Class Members who purchased "paid-delete." As a result, Personal Information of Plaintiffs and other Class Members who paid to have their information deleted remained on Defendants' system and was publicly leaked on the internet as part of the data breach. On information and belief, this information included personally-identifying information such as names, addresses, email addresses and payment information.

96. Upon information and belief, Defendants Avid Life Media, Inc. and/or Avid Dating Life, Inc. accept customer payments for services through credit and debit cards issued by members of the payment card industry ("PCI") such as Visa or MasterCard.

97. In 2006, the PCI members established a Security Standards Counsel ("PCI SSC") as a forum to develop PCI Data Security Standards ("PCI DSS") for increased security of payment processing systems.

98. The PCI DSS provides, "If you are a merchant that accepts payment cards, you are required to be compliant with the PCI Data Security Standard." Defendants Avid Life Media and Avid Dating Life are merchants that accept payment cards.

99. The PCI DSS requires a merchant to:

a. **Assess**—identify cardholder data, take inventory of IT assets and business processes for payment card processing, and analyze them for vulnerabilities that could expose cardholder data.

b. **Remediate**—fix vulnerabilities and do not store cardholder data unless needed.

c. **Report**—compile and submit required remediation validation records (if applicable) and submit compliance reports to the acquiring bank and card brands with which a merchant does business.

100. The PCI DSS also required Defendants to, among other things, comply with twelve data security standards that included installing and maintaining firewalls to protect data, protecting stored data, encrypting the transmission of cardholder and payment data and sensitive information across public networks, using and regularly updating antivirus software, developing and maintaining secure systems and applications, restricting physical access to cardholder data, tracking and monitoring all access to network resources and cardholder data, regularly testing security systems and processes, and maintaining a policy that addresses information security. Indeed, Defendants' duties were even higher than the PCI DSS and other basic industry standards due to the sensitive nature of the "Ashley Madison" website, the products and services that Defendants offered to the public, and the representations and promises made by Defendants.

101. Had Defendants complied with the PCI DSS and other basic industry standards governing data security, the Ashley Madison data breach could not have occurred.

102. Additionally, since 1995, the Federal Trade Commission ("FTC") has been studying the manner in which online entities collect and use personal information and safeguards to assure that online data collection practice is fair and provides adequate information privacy protection. The result of this study is the FTC Fair Information Practice Principles. The core principles are:

a. **Notice/Awareness--**Consumers should be given notice of an entity's information practices before any personal information is collected from them. This requires that companies explicitly notify of some or all of the following:

- Identification of the entity collecting the data;
- Identification of the uses to which the data will be put;
- Identification of any potential recipients of the data;
- The nature of the data collected and the means by which it is collected;
- Whether the provision of the requested data is voluntary or required; and
- The steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

b. **Choice/Consent--**Choice and consent in an online information-gathering sense means giving consumers options to control how their data is used with respect to secondary uses of information beyond the immediate needs of the information collector to complete the consumer's transaction.

c. **Access/Participation--**Access as defined in the Fair Information Practice Principles includes not only a consumer's ability to view the data collected, but also to

verify and contest its accuracy. This access must be inexpensive and timely in order to be useful to the consumer.

d. **Integrity/Security**--Information collectors should ensure that the data they collect is accurate and secure. They should improve the integrity of data by cross-referencing it with only reputable databases and by providing access for the consumer to verify it. Information collectors should keep their data secure by protecting against both internal and external security threats. They should limit access within their company to only necessary employees to protect against internal threats, and they should use encryption and other computer-based security systems to stop outside threats.

e. **Enforcement/Redress**--In order to ensure that companies follow the Fair Information Practice Principles, there must be enforcement measures. The FTC identifies three types of enforcement measures: self-regulation by the information collectors or an appointed regulatory body; private remedies that give civil causes of action for individuals whose information has been misused to sue violators; and government enforcement, which can include civil and criminal penalties levied by the government.

103. On information and belief, Defendants failed to adequately analyze their computer systems for vulnerabilities that could expose cardholder data and other Personal Information. On information and belief, Defendants knowingly stored highly sensitive information in an unencrypted format at the database level on their servers, in violation of accepted industry practices and FTC guidelines. Defendants failed remedy these and other vulnerabilities in their computer systems and thereby knowingly allowed third parties to obtain Plaintiffs and Class Members' Personal Information and release it onto the internet.

104. Additionally, on information and belief, Defendants unlawfully collected consumer financial data for marketing purposes beyond the needs of specific transactions, in order to accrue financial benefit at the risk and likelihood of compromising consumers' Personal Information.

105. As a result, Defendants allowed Personal Information to become compromised. This included information relating to thousands of consumers' credit cards and debit cards, including credit cards and debit cards of Plaintiffs and Class Members, as well as other highly confidential Personal Information.

106. Plaintiffs and Class Members are subject to continuing damage from having their Personal Information comprised as a result of Defendants' inadequate systems and failures. Such damages include, among other things, the amount paid to Defendants to perform a "paid-delete" which Defendants did not perform or performed inadequately; public humiliation, ridicule, divorce, extortion, loss of employment, and other catastrophic personal and professional harms; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendants' security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit/debit cards of Defendants' customers by identity thieves who wrongfully gained access to the Personal Information of Plaintiffs and Class Members.

107. In addition, and upon information and belief, Defendants were engaging in deceptive and fraudulent conduct by creating fake computer "hosts" or "bots", which were programmed to generate and send messages to male members.

108. While creating an account (and providing Personal Information to create a profile) was initially free, a user must make an additional payment and/or purchase "credits" from Ashley Madison in order to become a "full member" and send messages or otherwise interact with others on the site.

109. After a male member created an account, Defendants frequently caused computer generated messages to be sent by their "bots" to these new members. On information and belief Defendants' purpose in deploying the "bots" was to both create the false impression of a high level of activity by female users on the website, and to deceive male members into believing that real female members were interested in them so that the male members would spend money ("credits" purchased from Defendants and/or charges to "upgrade" their accounts), to interact with these fake "bot" accounts.

110. On information and belief, the vast majority of first purchases made on the Ashley Madison website by male members, constituting millions of individual payments and many millions of dollars, were made in response to messages sent by these "bot" accounts. In reality, the new members were being deceived into paying to chat with a computer.

111. On information and belief, many of the fake female profiles were in fact created by employees of Defendants or by persons paid by Defendants to create fake female profiles. In 2012, a former employee named Doriana Silva filed a lawsuit against Avid alleging that she developed a repetitive strain injury after being made to input as many as 1,000 fake female profiles (the "Silva Lawsuit").

112. The Silva Lawsuit alleged that "Ashley Madison — the dating site for married people seeking affairs — is riddled with fake profiles for women that encourage men to spend more money subscribing to the site[.]"[1] The Silva Lawsuit further alleged that the purpose of these profiles is to entice paying male members to join and spend money on the website, and the profiles "do not belong to any genuine members of Ashley Madison — or any real human beings at all."

113. The Ashley Madison site's Terms and Conditions have at various times referred, using vague, misleading and deceptive language, to "profiles" which may be in reference to the artificial bots. On information and belief, however, Defendants have withheld material information from Plaintiffs and the Class Members and have responded to questions raised regarding the "bots" by making numerous misleading and deceptive statements, such as that bots were created by criminal elements, were for "market research" or "entertainment purposes," when in fact the only purpose of the "bots" was to extract payment to Defendants from Plaintiffs and the Class Members under false pretenses.

114. On information and belief, on or about January 11, 2012, the California Attorney General contacted Defendants regarding allegations from a consumer that Defendants had committed fraud by using fake profiles to engage customers in conversations. On further information and belief, Defendant Biderman and others created and sent a misleading response to the Attorney General's inquiry blaming the fake profiles on "criminal elements."

115. Defendants' Ashley Madison website included numerous other deceptive and misleading functions designed to extract money from users without their knowledge. For example, Defendants also provided a purported "Priority Mail" function for messages which

[1] See http://www.businessinsider.com/ashley-madison-fake-profile-lawsuit-2013-11 (last accessed June 2, 2016).

roughly doubled the cost of sending messages. However, "Priority Mail" was set up as an "opt out" option, meaning that users would be charged for Priority Mail unless they affirmatively chose not to use it. The "opt out" option was deceptively concealed so that the vast majority of users would never know that it existed. None of these facts were disclosed in the site's Terms and Conditions.

CLASS ACTION ALLEGATIONS

116. Plaintiffs bring Count I and II of this action on their own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following nationwide classes:

> All persons in the United States who paid Defendants for "paid-delete" services prior to July 19, 2015, and whose data was released as a result of the data breach.
>
> All persons in the United States whose Personal Information was released as a result of the data breach and who have suffered or anticipate suffering damages, loss, and/or expenses accruing due to Defendants' security failures.
>
> All persons in the United States who paid Defendants for "credits", account upgrades, or otherwise paid to use Defendants' messaging systems.

117. Plaintiffs bring Counts III, IV, V, VI and VII of this action on their own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following nationwide classes, or in the alternative, on behalf of statewide classes consisting of consumers from the states of Alabama, Arizona, Arkansas, California, Colorado, Florida, Illinois, Louisiana, Maryland, Minnesota, Mississippi, Missouri, Nevada, North Carolina, New Jersey, Virginia and Washington:

> All persons who paid Defendants for "paid-delete" services prior to July 19, 2015, and whose data was released as a result of the data breach.
>
> All persons whose Personal Information was released as a result of the data breach and who have suffered or anticipate suffering damages, loss, and/or expenses accruing due to Defendants' security failures.

> All persons who paid Defendants for "credits", account upgrades, or otherwise paid to use Defendants' messaging systems.

118. Plaintiffs also bring Count VIII of this action for breach of the consumer fraud statutes of the states of Alabama, Arizona, Arkansas, California, Colorado, Florida, Illinois, Louisiana, Maryland, Minnesota, Mississippi, Missouri, Nevada, North Carolina, New Jersey, Virginia and Washington, and the consumer fraud statutes of similar states, on their own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of statewide consumer fraud sub-classes for each of said states, as follows:

> All persons who paid Defendants for "paid-delete" services prior to July 19, 2015, and whose data was released as a result of the data breach.
>
> All persons whose Personal Information was released as a result of the data breach and who have suffered or anticipate suffering damages, loss, and/or expenses accruing due to Defendants' security failures.
>
> All persons who paid Defendants for "credits", account upgrades, or otherwise paid to use Defendants' messaging systems.

119. Plaintiffs Nhung Truong and Gustavo Alfaro assert Count IX for violations of the California Customer Records Act on their own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class of California consumers, as follows:

> All California residents and domiciliaries whose Personal Information was released as a result of the data breach and who have suffered or anticipate suffering damages, loss, and/or expenses accruing due to Defendants' security failures.

120. Plaintiffs also bring Count X of this action on their own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of statewide consumer fraud sub-classes for violations of the data breach notice statutes of the states of Arizona, Arkansas, California, Colorado, Florida, Illinois, Louisiana, Maryland, Minnesota, Mississippi, Missouri,

North Carolina, New Jersey, Virginia and Washington, and the similar statutes of other states wherein Defendants transact business, as follows:

> All persons whose Personal Information was released as a result of the data breach and who have suffered or anticipate suffering damages, loss, and/or expenses accruing due to Defendants' security failures.

121. Excluded from each of the above Classes are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors.

122. The Class Members are so numerous that joinder of all Members is impracticable. The Class Members are geographically dispersed and number in the thousands or millions. Disposition of the claims of the proposed Classes in a class action will provide substantial benefits to both the parties and the Court.

123. The rights of each member of the proposed Classes were violated in a similar fashion based upon Defendants' uniform wrongful actions and/or inaction.

124. The following questions of law and fact are common to each proposed Class Member or Sub-Class Member and predominate over questions that may affect individual Class Members:

a. Whether Defendants failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' private and highly sensitive Personal Information;

b. Whether Defendants falsely promised that all evidence of usage and all personally identifiable information would be removed for Class Members who paid to exercise the "full delete" or "paid delete" option;

c. Whether a significant number of the apparent female profiles on the Ashley Madison website were in fact artificial "bots" created by Defendants;

d. Whether Defendants' purpose in creating and employing the "bots" was to extract payments from Plaintiffs and Class Members under false pretenses;

e. Whether Defendants complied with the PCI DSS and otherwise properly implemented its purported security measures to protect consumers' private financial information and other Personal Information from unauthorized capture, dissemination and misuse;

f. Whether Defendants took reasonable measures to determine the extent of the security breach after it first learned of the same;

g. Whether Defendants' delay in informing consumers of the security breach was unreasonable;

h. Whether Defendants' method of informing consumers of the security breach and their exposure to damages as a result of the same was unreasonable;

i. Whether Defendants engaged in a fraudulent scheme in violation of the RICO Statute, 18 U.S.C. §1962;

j. Whether Defendants' Ashley Madison Website Enterprise constituted an enterprise engaged in, or the activities of which affected, interstate or foreign commerce for purposes of the RICO statute, 18 U.S.C. §1962;

k. Whether Defendants conducted or participated in the conduct of the Ashley Madison Website Enterprise's affairs through a pattern of racketeering activities;

l. Whether Defendants knowingly participated in, devised, or intended to devise a scheme or plan to defraud, or a scheme or plan for obtaining money or

property by means of false or fraudulent pretenses, representations, promises, or omissions;

m. Whether the statements made or facts omitted as part of the scheme were material; that is, whether they had a natural tendency to influence, or were capable of influencing, a person to part with money or property;

n. Whether Defendants acted with the intent to defraud; that is, the intent to deceive or cheat;

o. Whether Defendants used, or caused to be used, the mails or interstate wire transmissions to carry out, or attempt to carry out, an essential part of the scheme

p. Whether Defendants' conduct violated the Stored Communications Act, 18 U.S.C. § 2702;

q. Whether Defendants breached an implied contract with Class Members;

r. Whether Defendants breached a contract or implied contract that all evidence of usage and all personally identifiable information would be removed for Class Members who paid to exercise the "full delete" or "paid delete" option;

s. Whether Defendants were negligent, and whether as a result of Defendants' negligence the Personal Information of the Plaintiffs and the Class was released in the data breach;

t. Whether Defendants concealed material facts or employed fraudulent, misleading or deceptive means in relation to Defendants use of "bots";

u. whether Defendants' advertisements, statements, and disclosures were false, misleading or reasonably likely to deceive;

v. Whether Defendants' conduct violated consumer fraud statutes; and

w. Whether Plaintiffs and other Class members are entitled to compensation, monetary damages, equitable relief and injunctive relief, and, if so, the nature and amount of such relief.

125. Plaintiffs' claims are typical of the claim of absent Class Members. Each of the Plaintiffs had their Personal Information released in the data breach, and each of the Plaintiffs paid for the "paid delete" option prior to the breach and/or made payments as a result of Defendants' fraudulent employment of "bots." If brought individually, the claim of each Class Member would necessarily require proof of the same material and substantive facts, and seek the same remedies.

126. Further, and in the alternative, Rule 23(c)(4) permits an action to be maintained as a class action with respect to only particular issues, and the common questions of law and fact set forth above raise issues which are appropriate for class treatment pursuant to Rule 23(c)(4).

127. The Plaintiffs are willing and prepared to serve the Court and the proposed Classes in a representative capacity. The Plaintiffs will fairly and adequately protect the interest of the Classes and have no interests adverse to, or which directly and irrevocably conflicts with, the interests of other Members of the Classes. Further, Plaintiffs have retained counsel experienced in prosecuting complex class action litigation.

128. Defendants have acted or refused to act on grounds generally applicable to the proposed Classes, thereby making appropriate equitable relief with respect to the Classes.

129. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual claims by the Class Members are impractical, as the costs of prosecution may exceed what any Class Member has at stake.

130. Members of the Classes are readily ascertainable through Defendants' records of the transactions they undertook.

131. Prosecuting separate actions by individual Class Members would create a risk of inconsistent or varying adjudications that would establish incomparable standards of conduct for Defendants. Moreover, adjudications with respect to individual Class Members would, as a practical matter, be dispositive of the interests of other Class Members.

132. Proposed class counsel are experienced in complex, class action litigation, have no conflicts of interest, and will zealously pursue the interests of the Proposed Class Members herein.

CAUSES OF ACTION

COUNT I

VIOLATIONS OF THE RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT, 18 U.S.C. §1962

133. Plaintiffs incorporate the above allegations by reference as if set forth herein.

134. This claim arises under 18 U.S.C. §1962(c) and (d), which provides in relevant part:

> (c) It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity . . . .
>
> (d) It shall be unlawful for any person to conspire to violate any of the provisions of subsection . . . (c) of this section.

135. At all relevant times, Defendants were "persons" within the meaning of 18 U.S.C. §1961(3), because each Defendant was "capable of holding a legal or beneficial interest in property." Defendants were associated with an illegal enterprise, as described below, and conducted and participated in that enterprise's affairs though a pattern of racketeering activity, as

defined by 18 U.S.C. §1961(5), consisting of numerous and repeated uses of interstate mail and wire communications to execute a scheme to defraud consumers in violation of 18 U.S.C. §1962(c).

136. At all relevant times, the Ashley Madison website constituted an "enterprise" within the meaning of 18 U.S.C. §1961(4), through which Defendants conducted the pattern of racketeering activity described herein. Defendants were each associated-in-fact with each other and other individuals and entities for a number of common and ongoing purposes with regard to the Ashley Madison website, including executing and perpetuating the illegal scheme, and constituted an "enterprise" within the meaning of 18 U.S.C. §1961(4), the activities of which affected interstate commerce.

137. Defendants engaged in a fraudulent scheme, common course of conduct and conspiracy to increase revenues and minimize losses for Defendants and their co-conspirators through the operation of the Ashley Madison website, and to conceal from the public and regulators that conspiracy.

138. Namely, Defendants engaged in a conspiracy to use the Ashley Madison website, in addition to its legitimate and legal business, to perpetuate an illegal scheme to conceal material information from its users and disseminate fraudulent information. This conduct included advertising and marketing misleading and fraudulent materials regarding Defendants' false "paid delete option" and Defendants' fraudulent and deceptive use of "bots" (the "Illegal Scheme"). As a direct result of their conspiracy and Illegal Scheme, Defendants were able to extract revenues in the amount of millions of dollars from Plaintiffs and the Class Members.

The Ashley Madison Website Enterprise

139. The Ashley Madison Website Enterprise is an ongoing and continuing organization consisting of legal entities, such as (at least) two corporations, as well as individuals

such as Defendant Biderman, the John Doe Defendants, as well as other managing executives, officers, employees and third party agents, associated for the common or shared purpose of defrauding Plaintiffs and the Class Members through deceptive and misleading tactics or materials in relation to the Ashley Madison website, and deriving profits from those activities.

140. Defendants Avid Life Media, Inc., Avid Dating Life, Inc., Noel Biderman and Doe Defendants #1 - #5 were associated-in-fact with each other and with other individuals and entities for a number of common and ongoing purposes, including executing and perpetuating the Illegal Scheme, and constituted an "enterprise" within the meaning of 18 U.S.C. §1961(4), the activities of which affected interstate commerce (the enterprises alleged in this and the previous paragraph are referred to collectively as the "Ashley Madison Website Enterprise").

141. Defendants Avid Life Media, Inc. and Avid Dating Life, Inc. are Canadian corporations that are not publicly traded and that have reporting obligations, protections and responsibilities unique to Canadian Law.

142. Defendant Noel Biderman is the former Chief Executive Officer of Avid Life Media, Inc. and may have held additional positions with Avid Life Media, Inc. and/or Avid Dating Life, Inc. Defendant Biderman and Doe Defendants #1 - #5 effectively controlled the operations of Defendants Avid Life Media, Inc. and Avid Dating Life, Inc.

143. Defendant Biderman's motives, goals and actions were distinct from and outside the normal scope of his employment as an executive and employee of Defendant Avid Life Media, Inc. Namely, on information and belief, Defendant Biderman possessed a significant ownership interest in Avid Life Media, Inc. and possessed a personal interest in concealing the true nature of the illicit activities of the Ashley Madison website.

144. On information and belief, Biderman hoped to sell his interest in the corporate defendants before the criminal conspiracy collapsed, and/or take those Defendants public, and thereby personally benefit. Therefore Biderman sought by any means to inflate the appearance of profitability of Ashley Madison and to conceal the illegal and fraudulent conspiracy occurring in relation to the Ashley Madison site.

145. On information and belief, Doe Defendants #1 - #5 similarly carried out their various distinct roles in the Ashley Madison Website Enterprise in furtherance of their own personal interests and outside of the regular scope and course of their agency or employment relationships with Avid Life Media, Inc. and/or Avid Dating Life, Inc. The specific roles played by Doe Defendants #1 - #5 in the structure of the Ashley Madison Website Enterprise have been concealed from the public and cannot be fully described without discovery on behalf of Plaintiffs and the Class.

146. Avid Life Media, Inc. is a parent corporation that conducts much of its business – legitimate and illegitimate – through a number of subsidiaries, each of which was a separate and distinct legal entity, including Defendant Avid Dating Life, Inc.

147. Defendants directed the affairs of the Ashley Madison Website Enterprise through, among other things, using Biderman and other executive officers of the corporate defendants to direct critical aspects of the Ashley Madison website. This included making false and deceptive public statements regarding the operations and security of the Ashley Madison Website.

148. The Ashley Madison Website Enterprise constituted an "enterprise" within the meaning of 18 U.S.C. §1961(4), as individuals and other entities associated-in-fact for the common purpose of engaging in Defendants' profit-making scheme.

149. The Ashley Madison Website Enterprise functions by offering a website with various social media services to the consuming public. Some these products are legitimate and non-fraudulent. However, Defendants, through the Ashley Madison Website Enterprise, have engaged in a pattern of racketeering activity which also involves a fraudulent scheme to increase revenue for the corporate Defendants and to provide personal gain and protect the interests of the personal Defendants.

150. The Ashley Madison Website Enterprise engages in and affects interstate commerce because it involves commercial activities across state boundaries, such as offering an accessible website across state boundaries for paid use by the public, as well as the marketing, promotion, and advertisement of said website throughout the United States, and the receipt of monies from the sale of the website's services.

151. Within the Ashley Madison Website Enterprise, there was a common communication network by which co-conspirators shared information on a regular basis. The Ashley Madison Website Enterprise used this common communication network for the purpose of defrauding Plaintiffs and the Class.

152. Each participant in the Ashley Madison Website Enterprise had a systematic linkage because there are corporate ties, contractual relationships, financial ties, and a continuing coordination of activities in furtherance of the Enterprise. Through the Ashley Madison Website Enterprise, Defendants engaged in consensual decision making to implement their fraudulent scheme and to function as a continuing unit for the common purpose of exacting revenues and market advantage. Furthermore, the Ashley Madison Website Enterprise functions as a continuing unit with the purpose of assisting with, perfecting and furthering their wrongful scheme.

153. While Defendants participate in, and are members of, the Ashley Madison Website Enterprise, they also have a separate and distinct existence.

154. Each Defendant exercised substantial control over the direction of the Ashley Madison Website Enterprise by:

a. The corporate defendants' use of their managing executives and officers to control the operations of the Ashley Madison website;

b. Defendant Biderman and the John Doe Defendants' use of their influence and position within the corporate defendants to carry out the Illegal Scheme;

c. Defendants' false representations regarding the safety of the Website and the security of the Personal Information provided by Plaintiffs and the Class Members;

d. Defendants' false and misleading statements regarding the data breach and the ongoing risk to Plaintiffs and the Class Members

e. Defendants' directing and designing the Website such that acceptance of the "paid delete" option did not delete all of Plaintiffs and the Class Members' Personal Information;

f. Defendants' directing and designing the website to employ "bots" to lure Plaintiffs and Class Members into making payments to interact with non-existent persons; and

g. Defendants' collecting of ill-gotten revenues and profits from Plaintiffs and the Class Members.

155. At all relevant times, each participant in the Ashley Madison Website Enterprise was aware of the scheme, was a knowing and willing participant in the scheme, and reaped revenues and/or profits therefrom.

156. The Ashley Madison Website is a separate and distinct entity created by Defendants and third party agents and vendors. The Enterprise consists of a structure of corporate and individual persons engaged in a conspiracy to employ the Ashley Madison website to carry out a fraudulent scheme.

157. Defendants have directed and controlled the ongoing organization necessary to implement their scheme and illicit business practices at meetings and through communications of which Plaintiffs cannot now know because all such information lies in Defendants' hands.

Pattern of Racketeering Activity

158. Defendants, each of whom is a person associated-in-fact with the Ashley Madison Website Enterprise, did knowingly, willfully, and unlawfully conduct or participate, directly or indirectly, in the affairs of the enterprise through a pattern of racketeering activity within the meaning of 18 U.S.C. §§1961(1), 1961(5) and 1962(c). The racketeering activity was made possible by Defendants' regular and repeated use of the facilities, services, distribution channels, and employees of the Ashley Madison Website Enterprise.

159. Defendants each committed multiple "Racketeering Acts," as described below.

160. The Racketeering Acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims, and methods of commission. Further, the Racketeering Acts were continuous, occurring on a regular, and likely daily, basis throughout a time period continuing at least through July of 2015.

161. Defendants participated in the operation and management of the Ashley Madison Website Enterprise by directing its affairs, as described above.

162. In devising and executing the Illegal Scheme, Defendants committed acts constituting indictable offenses under 18 U.S.C. §§1341 and 1343, in that they devised and knowingly carried out a material scheme or artifice to defraud Plaintiffs and the Class or to obtain money from Plaintiffs and the Class by means of materially false or fraudulent pretenses, representations, promises, or omissions of material facts. For the purpose of executing the Illegal Scheme, Defendants committed these Racketeering Acts, which number in the thousands or millions, intentionally and knowingly with the specific intent to advance the Illegal Scheme.

163. Defendants used thousands or millions of mail and interstate wire communications to create and manage their fraudulent scheme through virtually uniform misrepresentations, concealments and material omissions, described above, which were disseminated via false and misleading marketing materials and advertisements, as well via false and misleading statements posted on Defendants' Ashley Madison website.

164. Defendants' fraudulent use of the mail and wires included the following items and communications sent by Defendants to each other, Plaintiffs and third parties via interstate wire, and/or other interstate electronic media:

a. Defendants' false, fraudulent, misleading and deceptive statements on the Ashley Madison website and elsewhere that the "paid delete" option would "remove all traces of your usage" of the Ashley Madison website and ensure that all personally identifiable information related to the consumer would be removed, when Defendants knew this was untrue and that Plaintiffs and the Class would rely on this material misrepresentation;

b. Fraudulent communications from "bots", programmed by Defendants, to Plaintiffs and Class Members to induce them to believe they were interacting with real persons, rather than computer programs, and to pay credits to do so, all in order to obtain payments under false pretenses;

c. Defendants' fraudulent and deceptive statements regarding the existence and source of the "bots" on the Ashley Madison website;

d. Documents relating to Defendants' collection of ill-gotten revenues and profits from Plaintiffs and the Class from the sale of their "services";

e. Other documents and things.

165. On information and belief, Defendants have communicated by U.S. mail and by interstate electronic mail, including through the internet, with various subsidiaries, regional offices, affiliates, divisions and other entities in furtherance of their scheme.

166. Defendants and third parties have exclusive custody or control over the records reflecting the precise dates and time of the mailings and wire transmissions described above.

167. Defendants' uniform acts of concealment and omissions were knowing and intentional and made for the purpose of deceiving the Plaintiffs and Class Members, selling worthless services, and obtaining revenues and profits as a result thereof.

168. Defendants either knew or recklessly disregarded that their misrepresentations and omissions were material and were relied upon by Plaintiffs and Class Members as shown by their payments to Defendants for worthless services, and resulting injury.

169. The Ashley Madison Website Enterprise was created and/or used as a tool to carry out the elements of Defendants' illicit scheme and pattern of racketeering activity.

170. The members of the RICO enterprise all had the common purpose to increase and maximize revenues and profits for Defendants through the fraudulent conduct described above.

171. Defendants knowingly and intentionally made the aforesaid misrepresentations, acts of concealment and failures to disclose so as to deceive Plaintiffs and Class Members. Defendants either knew or recklessly disregarded that these were material misrepresentations and omissions, and Plaintiffs and the Class relied on the misrepresentations and omissions as set forth herein.

172. Defendants have obtained money and property belonging to Plaintiffs and the Class as a result of these statutory violations. Plaintiffs and other Class Members have been injured in their business or property by Defendants' overt acts of mail and wire fraud.

173. In violation of 18 U.S.C. §1962(d), Defendants conspired to violate 18 U.S.C. §1962(c), as described herein. Various other persons, not named as defendants in this Complaint, have participated as co-conspirators with Defendants in these offenses and have performed acts in furtherance of the conspiracy.

174. Each Defendant aided and abetted violations of the above laws, thereby rendering them indictable as a principal in the 18 U.S.C. §§1341 and 1343 offenses pursuant to 18 U.S.C. §2.

175. Plaintiffs and the Class Members have been injured in their property by reason of Defendants' violations of 18 U.S.C. §1962(c) and (d), including the purchase price of the Defendants' services. In the absence of Defendants' violations of 18 U.S.C. §1962(c) and (d), Plaintiffs and the Class would not have incurred these costs and expenses.

176. Plaintiffs and the Class Members relied, to their detriment, on Defendants' fraudulent misrepresentations and omissions, which were made by virtually uniform

representations or omissions made through the interstate mails or interstate wire or electronic communications. Plaintiffs' and the Class Members' reliance is evidenced by their purchases.

177. Plaintiffs' and the Class Members' injuries were directly and proximately caused by Defendants' racketeering activity.

178. Defendants knew Plaintiffs and the Class Members relied on their representations and omissions. Defendants knew that consumers would incur substantial costs as a result.

179. Under the provisions of 18 U.S.C. §1964(c), Plaintiffs are entitled to bring this action and to recover treble damages, *i.e.* three times their actual damages, the costs of bringing this suit and reasonable attorneys' fees.

RICO Conspiracy

180. Defendants have not undertaken the practices described herein in isolation, but as part of a common scheme and conspiracy.

181. Defendants have engaged in a conspiracy to increase or maintain revenues and/or minimize losses of revenues or profits for Defendants and their unnamed co-conspirators.

182. The objects of the conspiracy are: (a) to convince the public to use the Ashley Madison Website and pay for valueless services, such as Defendants' "paid delete" option or to interact with "bots"; (b) to maximize profits and revenues for all Defendants; and/or (c) to conceal the conspiracy from the public to protect the interests of Defendants.

183. To achieve these goals, Defendants knowingly hid from the general public the flaws in their network security measures and their inability to protect the Personal Information provided by Plaintiffs and the Class Members. Defendants have also agreed to participate in other illicit and fraudulent practices, all in exchange for agreement to, and participation in, the conspiracy.

184. Each Defendant and member of the conspiracy, with knowledge and intent, has agreed to the overall objectives of the conspiracy and participated in the common course of conduct to commit acts of fraud in relation to the Ashley Madison website.

185. Indeed, for the conspiracy to succeed, each Defendant and co-conspirator had to agree to implement and use the similar devices and fraudulent tactics against their intended targets.

186. As a result of Defendants' Illegal Scheme and conspiracy, Plaintiffs and the Class Members purchased "services" which had little or no monetary value, including paying for Defendants' "paid-delete" service or purchasing credits which were used to interact with "bots." But for Defendants' Illegal Scheme, no one would have purchased these services. Therefore, the damages that Defendants caused Plaintiffs and the Class may be measured, at a minimum, by each dollar paid for the "paid-delete" service or for "credits" which were used or could have been used to interact with "bots."

WHEREFORE Plaintiffs and the Class Members pray for Judgment in their favor and against Defendants on this Count I of their Consolidated Class Action Complaint; for actual and compensatory damages; for treble damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT II

VIOLATION OF THE FEDERAL STORED COMMUNICATIONS ACT, 18 U.S.C. § 2702

187. Plaintiffs repeat, reallege, and incorporate the preceding paragraphs in this Complaint as if fully set forth herein.

188. The Stored Communications Act ("SCA") contains provisions that provide consumers with redress if a company mishandles their electronically stored information. The

SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and proprietary information." S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 at 3557.

189. Section 2702(a)(1) of the SCA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

190. The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* at § 2510(15).

191. Through their servers (which are under Defendants' control), Defendants provide an "electronic communication service to the public" within the meaning of the SCA because Defendants' services allows members of Ashley Madison to submit their Personal Information to the Ashley Madison website and allows members to communicate electronically with other members through Defendants' servers. Furthermore, Defendants provide an "electronic communication service to the public" within the meaning of the SCA because Defendants provide consumers at large with credit and debit card payment processing capability that enables them to send or receive wire or electronic communications concerning their private financial information to transaction managers, card companies, or banks.

192. By failing to take commercially reasonable steps to safeguard sensitive Personal Information, even after Defendants were aware that customers' Personal Information had been compromised and were further aware that the Personal Information was going to be publicly

released, Defendants knowingly divulged customers' private communications and Personal Information, in violation of the SCA.

193. Furthermore, Defendants knowingly retained information which they had promised to delete under the "paid delete" function, despite the reliance of Plaintiffs and the Class that such information had been deleted, and the despite the risk that such information would ultimately be divulged in a data breach or otherwise. Defendants thereby knowingly divulged customers' private communications and Personal Information, in violation of the SCA.

194. Section 2702(a)(2)(A) of the SCA provides that "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

195. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communication system." 18 U.S.C. § 2711(2).

196. An "electronic communications systems" is defined by the SCA as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(4).

197. Through their servers, Defendants provide remote computing services to the public within the meaning of the SCA.

198. By failing to take commercially reasonable steps to safeguard sensitive private financial information, Defendants have knowingly divulged customers' Personal Information that was carried and maintained on Defendant's remote computing service.

199. As a result of Defendants' conduct described herein and its violations of Section 2702(a)(1) and (2)(A), Plaintiffs and Class Members have suffered injuries and damages as alleged herein. Plaintiffs, on their own behalf and on behalf of the putative Classes, seek an order awarding themselves and the Class the maximum statutory damages available under 18 U.S.C. § 2707.

WHEREFORE Plaintiffs and the Class Members pray for Judgment in their favor and against Defendant on this Count II of their Consolidated Class Action Complaint; for actual and compensatory damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT III
NEGLIGENCE AND NEGLIGENCE *PER SE*

200. Plaintiffs repeat, reallege, and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

201. Upon coming into possession of Plaintiffs' and the Class Members' Personal Information, *i.e.*, private, non-public, sensitive financial and personal information, Defendants had (and continue to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen. Defendants owed a duty to prevent precisely the type of harm that occurred as a result of the data breach.

202. Furthermore, Defendants assumed a heightened duty to exercise care in safeguarding and protecting the information provided by users, based on Defendants' affirmative

promises to Plaintiffs and the Class that Defendants utilized heightened care and security measures.

203. Defendants had a duty to timely disclose to Plaintiffs and the Class Members that a data breach had occurred and their Personal Information had been compromised, or was reasonably believed to be compromised.

204. Defendants also had a duty to put into place internal policies and procedures designed to detect and prevent the theft or dissemination of Plaintiffs' and Class Members' Personal Information.

205. Defendants owed duties to Plaintiffs and the Class Members under the Stored Communications Act regarding the handling of electronically stored information, as set forth in Count II, infra, including the duty to take commercially reasonable steps to safeguard sensitive Personal Information and to not knowingly disclose that information.

206. Defendants owed duties to Plaintiffs and the Class Members under the guidelines issued by the FTC, discussed above, including the duty to ensure that the collected data is securely maintained and that proper notice of the breach be provided to Plaintiffs and the Class Members.

207. Defendants, by and through their above negligent acts and/or omissions, breached their duties to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding their Personal Information which was in Defendants' possession, custody, and control.

208. Defendants, by and through their above negligent acts and or omissions, further breached their duty to Plaintiffs and Class Members by failing to put into place internal policies

and procedures designed to detect and prevent the unauthorized dissemination of Plaintiffs and Class Members' Personal Information.

209. Defendants, by and through their above negligent acts and or omissions, breached their duty to timely disclose the fact that Plaintiffs and Class Members' Personal Information had been or was reasonably believed to be have been compromised.

210. Defendants' breach of duties owed to Plaintiffs and the Class Members under the Stored Communications Act and under the guidelines and policies issued by the Federal Trade Commission constitute negligence per se.

211. But for Defendants' negligent and wrongful breach of their duties owed to Plaintiffs and Class Members, their Personal Information would not have been compromised.

212. Plaintiffs' and Class Members' Personal Information was compromised and/or stolen as a direct and proximate result of Defendants' breach of their duties as set forth herein.

213. As a direct and proximate result of Defendants' acts and omissions, Plaintiffs and Class Members have suffered injuries and damages as alleged herein.

214. The Defendants' conduct was undertaken in bad faith, with malice, and/or was willful and wanton and in reckless and conscious disregard of the rights of the Plaintiffs and the Class Members, which entitles the Plaintiffs and Class Members to be awarded punitive damages or exemplary damages in a amount sufficient to punish and deter Defendants and also to deter other entities and persons from similar conduct in the future.

WHEREFORE Plaintiffs and Class Members pray for Judgment in their favor and against Defendants on this Count III of their Consolidated Class Action Complaint; for actual and compensatory damages; for punitive or exemplary damages; for injunctive relief; for costs,

expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT IV
BREACH OF IMPLIED CONTRACT – DATA BREACH

215. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

216. Plaintiffs and Class Members were required to provide Defendants with their Personal Information in order to register with Defendants' website, utilize Defendants' "paid delete" service and/or to facilitate credit card and/or debit card transactions.

217. Implicit in this requirement was a covenant requiring Defendants to take reasonable efforts to safeguard this information and promptly notify Plaintiffs and Class Members in the event their Personal Information was compromised.

218. Similarly, it was implicit that Defendants would not disclose Plaintiffs' and the Class Members' Personal Information.

219. Notwithstanding their obligations, Defendants knowingly failed to safeguard and protect Plaintiffs' and Class Members' Personal Information. To the contrary, Defendants allowed this information to be disseminated to unauthorized third parties.

220. Defendants' above wrongful actions and/or inactions breached their implied contracts with Plaintiffs and Class Members, which in turn directly and/or proximately caused Plaintiffs and Class Members to suffer substantial injuries, as described above.

WHEREFORE Plaintiffs and Class Members pray for Judgment in their favor and against Defendants on this Count IV of their Consolidated Class Action Complaint; for actual and compensatory damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT V
BREACH OF CONTRACT – PAID DELETE

221. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

222. Defendants Avid Life Media and Avid Dating Life promised Plaintiffs and the Class Members, for a fee of approximately $19, to delete any Personal Information, including "all traces" of Plaintiffs' usage and all personally identifiable information in Defendants' possession.

223. Plaintiffs Brian Farr, Nhung Truong, Gustavo Alfaro and John Hiles III, and numerous other Class Members, accepted Defendants' offer and paid for the paid delete option.

224. The contract or implied contract as to each Plaintiff and Class Member was supported by mutual consideration, namely Defendants' promise and Plaintiffs and the Class Members' payments for fulfillment of that promise.

225. On information and belief, Defendants broke their promise, and did not delete all of Plaintiffs and the Class Member's information in Defendants' possession, even after the payment by Plaintiffs and Class Members. As a direct result, the Personal Information was obtained by hackers and released on the internet.

226. Plaintiffs and Class Members have been damaged thereby in the amount paid to the Defendants to perform a "paid-delete," interest on said amount, and in the amount of other losses as previously stated.

WHEREFORE Plaintiffs and the Class Members pray for Judgment in their favor and against Defendants on this Count V of their Consolidated Class Action Complaint; for actual and compensatory damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT VI
UNJUST ENRICHMENT

227. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

228. Plaintiffs and Class Members conferred a monetary benefit on Defendants in the form of monies paid for the purchase of the "paid delete" service from Defendants prior to the Defendants' data breach.

229. Plaintiffs and Class Members also conferred a monetary benefit on Defendants in the form of monies paid to send messages to artificial "bots" created by Defendants to appear to be human beings rather than computer programs.

230. Defendants appreciate or have knowledge of the benefits conferred directly upon them by Plaintiffs and Class Members.

231. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Plaintiffs were paying for worthless services. Furthermore, Defendants should not be permitted to retain the money relating to the "paid delete" function because Defendants failed to provide adequate safeguards and security measures to protect Plaintiffs' and Class Members' Personal Information.

232. As a result of Defendants' conduct as set forth in this Complaint, Plaintiffs and Class Members suffered damages and losses as stated above, including monies paid for Defendants' services that Plaintiffs and Class Members would not have purchased had Defendants disclosed the material facts.

233. The financial benefits derived by Defendants rightfully belong to Plaintiffs and the Class Members.

234. It would be inequitable under established unjust enrichment principles in the District of Columbia and all of the 50 states for Defendants to be permitted to retain any of the financial benefits derived from Defendants' unlawful conduct as set forth in this Complaint.

235. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class Members all unlawful or inequitable proceeds received by Defendants, and/or a constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiffs and the Class.

236. Plaintiffs further state, and in the alternative, that Plaintiffs and the Class Members have no adequate remedy at law.

WHEREFORE Plaintiffs and the Class Members pray for Judgment in their favor and against Defendants on this Count VI of their Consolidated Class Action Complaint; for restitution in the amount of all funds paid for the "paid delete" option and to purchase credits or send messages to "bots"; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT VII
NEGLIGENT MISREPRESENTATION

237. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

238. Defendants falsely represented to Plaintiffs and the Class Members that Defendants would perform a "full delete" of their Personal Information that, among other things, would "remove all traces of your usage".

239. Defendants falsely represented to the Plaintiffs and Class Members that communications received by Plaintiffs and Class Members on the Ashley Madison website were from other human members as opposed to "bots".

240. Defendants also falsely represented that the cost to read and/or send a message was five credits and failed to disclose to full members, either in the Terms and Conditions or elsewhere on the site, that the "priority mail" option, which cost an additional five credits, was set as the default option on members' accounts.

241. Plaintiffs and the Class Members did not know that Defendants had made these misrepresentations and omissions and reasonably believed Defendants' misrepresentations to be true.

242. Plaintiffs and the Class Members reasonably relied on Defendants' misrepresentations in signing up for AshleyMadison.com and in purchasing credits to communicate with other members. No reasonable person would have paid to send a message to a "bot."

243. Defendants knew or should have known that their representations that the "full delete" option would "remove all traces of your usage" were substantially false and not what they represented it to be.

244. Defendants knew or should have known that their representations, including that the website provided interaction with "real like-minded people", were substantially false, and that in fact millions of messages and chats being sent were computer generated and sent from "bot" accounts and did not provide interaction with real members.

245. Defendants knew or should have known that their representations that the cost of reading/receiving messages was "five credits" was not what they represented it to be, where the site defaulted to charging full members ten credits for sending messages and concealed the "opt out" option for "Priority Mail."

246. Defendants had a duty to disclose the true facts regarding the "paid delete" option and "bot" accounts, and the true facts regarding the cost of messages and/or a duty to not affirmatively misrepresent these facts. Defendants breached these duties.

247. As a result of Defendants' breaches, Plaintiffs and the Class Members were damaged.

248. Defendants' conduct was done in bad faith, with malice, and/or was willful and wanton and in reckless disregard of the rights of the Plaintiffs and the Class Members, which entitles the Plaintiffs and Class Members to be awarded punitive damages or exemplary damages in a amount sufficient to punish and deter Defendants and also to deter other entities and persons from similar conduct in the future.

WHEREFORE Plaintiffs and the Class Members pray for Judgment in their favor and against Defendants on this Count VII of their Consolidated Class Action Complaint; for actual and compensatory damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT VIII
VIOLATION OF CONSUMER FRAUD AND PROTECTION ACTS

249. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

250. This Count is brought pursuant to the consumer fraud and protection acts of the States of Alabama, Arizona, Arkansas, California, Colorado, Florida, Illinois, Louisiana, Maryland, Minnesota, Mississippi, Missouri, Nevada, North Carolina, New Jersey, Virginia and Washington, and the similar laws of the other states wherein Defendants perform business, as follows:

- Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1 *et seq.*
- Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1521, *et seq.*
- Arkansas Deceptive Trade Practices Act, Ark. Code Ann. § 4-88-101 *et seq.*
- California Consumers Legal Remedies Act, California Civil Code §1750, *et seq.*; California Unfair Competition Law, California Business and Professions Code §17200, *et seq.*; and California False and Misleading Advertising Law, California Business and Professions Code §17500, *et seq.*
- Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-101, *et seq.*
- Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*
- Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*
- Louisiana Unfair Trade Practices and Consumer Protection Act ("LUTPA") La. Rev. Stat. Ann. § 51:1405 *et seq.*
- Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-101 *et seq.*
- Minnesota Consumer Fraud Act, Minn. Stat. §§325F.68-325F.69 *et seq.*
- Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1, *et seq.*
- Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.020 *et seq.*
- Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 41.600 *et seq.* and Nev. Rev. Stat. §§ 598.0915-598.0925
- New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56-8-19, *et seq.*
- North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1 *et seq.*
- Virginia Consumer Protection Act, Va. Code § 59.1-196 *et seq.*
- Washington Consumer Protection Act, Rev. Code Wash. Ann. § 19.86.010, *et seq.*

251. The above statutes bar fraud, false pretenses, false promises, misrepresentations, unfair practices and the concealment of material facts in connection with the sale or advertisement of services to consumers, and permit private actions to be brought by consumers who are injured by such consumer fraud or unfair trade practices.

252. Plaintiffs and the Class Members purchased services from Defendants' Ashley Madison website. Plaintiffs purchased Defendants' services for their own personal, household use as consumers, and not for resale.

253. At all relevant times, Plaintiffs and other Class Members were purchasers and consumers within the meaning and scope of the above consumer fraud statutes.

254. At all relevant times, Defendants conducted significant trade and commerce in the above states and in the other states of the United States of America.

255. Defendants, individually and/or jointly, by and through their employees, agents, apparent agents, liaisons, and/or sales representatives, engaged in concealment, suppressions, and/or omissions, misrepresentations, unlawful schemes and unfair courses of conduct intended to induce the Plaintiffs and Class Members to purchase Defendants' worthless services through one or more of the following unfair and/or deceptive acts and/or practices:

a. Defendants' fraudulent and/or misleading and deceptive omissions and misrepresentations regarding security measures utilized to protect customers' Personal Information and the extent of the breach of those security measures;

b. Omitting, suppressing, and/or concealing material facts regarding the safety of the website and the security of the Personal Information provided by Plaintiffs and the Class Members, such as claiming that Defendants had received a "Trusted Security Award" which, according to published reports, does not exist;

c. Defendants' false and/or misleading and deceptive statements regarding the data breach and the ongoing risk to Plaintiffs and the Class Members, including the statement published on Ashley Madison's website on July 20, 2015;

d. Defendants' false and/or misleading and deceptive statements on the Ashley Madison website and elsewhere that the "paid delete" option would delete all Personal Information and "remove all traces of your usage" from the Ashley Madison website;

e. Defendants' use of "bots", programmed by Defendants to induce Plaintiffs and the Class Members to believe they were interacting with real persons and to pay credits to do so under false pretenses; and

f. Omitting, suppressing, and/or concealing the material fact that all messages were sent by "Priority Mail" by default and on an "opt out basis," for an increased cost of credits, which was not disclosed by Defendants.

256. The facts which Defendants misrepresented, omitted, suppressed, and/or concealed as alleged in the preceding paragraphs were material in that they concerned facts that would have been important to a reasonable consumer in making a decision whether to purchase Defendants' services.

257. Defendants' conduct as alleged in the preceding paragraphs was unfair in that, among other things, it (1) offended public policy; (2) it was immoral, unethical, oppressive, and/or unscrupulous; and/or (3) it caused substantial economic injury to consumers, namely Plaintiffs and the Class Members.

268. Defendants intended for Plaintiffs and Class Members to purchase Defendants' services in reliance upon Defendants' unfair and/or deceptive acts and/or practices in the

marketing, promotion, and sale of their services. Defendants' unfair, false, misleading and/or deceptive statements and actions were intended to deceive and induce Plaintiffs and the Class Members' reliance on Defendants' misrepresentations that their personal and financial information was secure.

269. As a direct and proximate result of Defendants' unfair and/or deceptive acts and/or practices, Plaintiffs and Members of the Class suffered actual damages when their Personal Information was leaked in the data breach, as well as when they paid for Defendants' worthless services.

270. Defendants' unfair and/or deceptive acts and/or practices were outrageous due to Defendants' evil motive and/or reckless indifference to the rights of others; and committed with complete indifference to and conscious disregard for Plaintiffs and the Class Members' rights, entitling Plaintiffs and the Class to punitive damages.

271. Plaintiffs, individually and on behalf of the putative Classes, seek an order requiring Defendants to pay monetary and punitive damages for the conduct described herein; credit card fraud monitoring services for Plaintiffs and Members of the putative Classes; and the reasonable attorney's fees and costs of suit of Plaintiffs and Class Members; together with all such other and further relief as may be just.

WHEREFORE Plaintiffs and Class Members pray for Judgment in their favor and against Defendants on this Count VIII of their Consolidated Class Action Complaint; for actual and compensatory damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT IX

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT

272. Plaintiffs Nhung Truong and Alfaro Gustavo repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

273. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted the Customer Records Act, California Civil Code §1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

274. A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. This disclosure shall be performed in the most expedient time possible and without unreasonable delay. See California Civil Code section 1798.82.

275. As described above, Defendants failed to implement and maintain reasonable security procedures and practices to protect the Plaintiffs and Class Members' Personal Information, including Plaintiffs Nhung Truong and Alfaro Gustavo and those Class Members who reside in California, and thereby violated California Civil Code section 1798.81.5. Furthermore, Defendants failed to provide notice to the Class as required by California Civil Code section 1798.82.

276. By violating the California Customer Records Act, Defendants are liable to the

Plaintiffs and Class Members for damages under California Civil Code section 1798.84(b).

277. Because Defendants "violate[], proposes to violate, or has violated," the California Customer Records Act, Plaintiffs and the Class Members are entitled to injunctive relief under California Civil Code section 1798.84(e).

278. In addition, Defendants' violations of the Customer Records Act constitute unlawful acts or practices under California's Unfair Competition Law, California Business and Professions Code sections 17200, et seq., which provides for restitution damages, and grants the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

279. Accordingly, Plaintiffs request that the court enter an injunction that requires Defendants to implement reasonable security procedures and practices, as required by California law.

280. For the reasons set forth above, the Plaintiffs and Class Members seek all remedies available under the California Customer Records Act and the California Unfair Competition Law, including but not limited to, restitution, damages, equitable relief, including injunctive relief, reasonable attorneys' fees and costs, and all other relief allowed under applicable law.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count IX of their Consolidated Class Action Complaint; for actual and compensatory damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT X

VIOLATION OF STATE DATA BREACH NOTIFICATION STATUTES

281. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

282. The Ashley Madison website data breach constitutes a breach of Defendants' computer security systems within the meaning of the state data breach notifications statutes listed below, and the data accessed in the breach was protected and covered by the below listed statutes.

283. Defendants unreasonably delayed notification of the data breach, including the unauthorized access and theft, after Defendants knew or should have known that the data breach had occurred.

284. On information and belief, although Defendants were aware of the data breach on July 12, 2015 or earlier, Defendants did not disclose or notify the public or Ashley Madison members of the data breach until after it was publicly announced by the hackers and referenced in on-line media on July 19, 2015.

285. Defendants failed to inform the public of the data breach during this time even though Defendants knew or should have known of its occurrence and the attendant unauthorized access, theft and dissemination of the Plaintiffs and Class Members' highly confidential Personal Information.

286. On or around July 20, 2015, Defendants began to make public statements regarding the data breach, however these statements were misleading and incomplete and downplayed the significance of the Data Breach and its threat to Plaintiffs and Class Members, all as set forth above. Further, although Defendants were in possession of the email addresses of the Plaintiffs and Class Members, Defendants failed to provide direct notice to the Plaintiffs and

Class Members that the data breach had occurred and, on information and belief, have never done so.

287. Defendants failed to disclose to Consumer Plaintiffs and the other Class Members, without unreasonable delay and in the most expedient time possible, the breach and the unauthorized access and theft of Plaintiffs and Class Members' Personal Information when Defendants knew, should have known, or reasonably believed that such information had been compromised. On information and belief, no law enforcement agency instructed Defendants to withhold notification and disclosure of the Data Breach.

288. As a result of Defendants' failure to notify in the statutorily prescribed time periods, Plaintiffs and the Class Members suffered the harm alleged above.

289. Had Defendants provided timely and accurate notice, Plaintiffs and Class Members could have taken steps to mitigate the direct harm suffered as a result of Defendants' unreasonable and untimely delay in providing notice.

290. Defendants' failure to notify Consumer Plaintiffs and the other Class Members violated the following state data breach notification statutes, and the similar statutes of other states wherein Defendants transact business:

- Arizona – Ariz. Rev. Stat. § 44-7501
- Arkansas - Ark. Code § 4-110-101 *et seq.*
- California - Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.*
- Colorado - Colo. Rev. Stat. § 6-1-716
- Florida - Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
- Illinois - 815 ILCS §§ 530/1 to 530/25
- Louisiana - La. Rev. Stat. §§ 51:3071 *et seq.*, 40:1300.111 to .116

- Maryland - Md. Code Com. Law §§ 14-3501 *et seq.*, Md. State Govt. Code §§ 10-1301 to -1308
- Minnesota - Minn. Stat. §§ 325E.61, 325E.64
- Mississippi - Miss. Code § 75-24-29
- Missouri - Mo. Rev. Stat. § 407.1500
- New Jersey - N.J. Stat. § 56:8-161, -163
- North Carolina - N.C. Gen. Stat §§ 75-61, 75-65
- Virginia - Va. Code § 18.2-186.6, § 32.1-127.1:05, § 22.1-20.2
- Washington - Wash. Rev. Code § 19.255.010, 42.56.590, 2015 H.B. 1078, Chapter 65

283. Consumer Plaintiffs and the other members of the Class seek all remedies available under the applicable state data breach notification statutes, including but not limited to damages as alleged above, equitable relief, injunctive relief and reasonable attorneys' fees, and costs, as provided by law.

WHEREFORE Plaintiffs and Class Members pray for Judgment in their favor and against Defendants on this Count X of their Consolidated Class Action Complaint; for actual and compensatory damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

JURY TRIAL DEMAND

Plaintiffs and Class Members demand a jury trial as to all claims and issues triable of right by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Members of the proposed Classes pray that this Honorable Court do the following:

A. Certify the matter as a class action pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class Members;

B. Designate Plaintiffs as representatives of the Class and the undersigned counsel as Class Counsel;

C. Award Plaintiffs and the Class compensatory, punitive and treble damages in an amount to be determined by the trier of fact;

D. Award Plaintiffs and the Class statutory interest and penalties;

E. Award Plaintiffs and the Class appropriate injunctive and/or declaratory relief;

F. Award Plaintiffs and the Class their costs, prejudgment interest, and attorney fees; and

G. Grant such other relief as is just and proper.

Date: June 3, 2016

Respectfully Submitted,

THE DRISCOLL FIRM, P.C.

By: */s/ John J. Driscoll*

John J. Driscoll (54729MO)
Christopher J. Quinn (41883MO)
Gregory G. Pals (48820MO)
211 N. Broadway, 40th Floor
St. Louis, Missouri 63102
Tel.: (314) 932-3232
Fax: (314) 932-3233
john@thedriscollfirm.com
chris@thedriscollfirm.com
greg@thedriscollfirm.com

W. Lewis Garrison, Jr.
Christopher B. Hood

Taylor C. Bartlett
HENINGER GARRISON DAVIS, LLC
2224 1st Avenue North
Birmingham, Alabama 35203
Tel.: (205) 326-3336
Fax: (205) 326-3332
wlgarrison@hgdlawfirm.com
chood@hgdlawfirm.com
taylor@hgdlawfirm.com

James F. McDonough, III
HENINGER GARRISON DAVIS, LLC
3621 Vinings Slope, Suite 4320
Atlanta, Georgia 30339
Tel.: (404) 996-0869
Fax: (205) 326-3332
jmcdonough@hgdlawfirm.com

Plaintiffs' Interim Co-Lead Counsel

Douglas P. Dowd (29240MO)
William T. Dowd (39648MO)
Alex R. Lumaghi (56569MO)
DOWD & DOWD, P.C.
211 North Broadway, Suite 4050
St. Louis, Missouri 63102
Tel.: (314) 621-2500 Fax: (314) 621-2503
doug@dowdlaw.net
bill@dowdlaw.net
alex@dowdlaw.net

Plaintiffs' Interim Liaison Counsel

John Arthur Eaves, Jr.
JOHN ARTHUR EAVES
ATTORNEYS AT LAW
101 North State Street
Jackson, Mississippi 39201
Tel.: (601) 355-7961
Fax: (601) 355-0530
johnjr@eaveslaw.com

Gary F. Lynch
Jamisen A. Etzel
CARLSON LYNCH SWEET &
KILPELA, LLP

1133 Penn Ave., 5th floor
Pittsburgh, Pennsylvania 15222
Tel.: (412) 322-9243
Fax: (724) 656-1556
glynch@carlsonlynch.com
jetzel@carlsonlynch.com

Thomas A. Zimmerman, Jr.
ZIMMERMAN LAW OFFICES, P.C.
77 West Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020
tom@attorneyzim.com

Julian A. Hammond
Ari Cherniak
Polina Pecherskaya
HAMMONDLAW, P.C.
1180 S. Beverly Drive, Suite 610
Los Angeles, CA 90035
(310) 601-6766
(310) 295-2385 (Fax)
jhammond@hammondlawpc.com
acherniak@hammondlawpc.com
ppecherskaya@hammondlawpc.com

Katrina Carroll
Kyle Alan Shamberg
LITE DEPALMA GREENBERG
211 W. Wacker Drive, Ste. 500
Chicago, IL 60606
312-750-1591
Fax: 312-212-5919
kcarroll@litedepalma.com
kshamberg@litedepalma.com

Plaintiffs' Interim Executive Committee

CERTIFICATE OF SERVICE

I hereby certify that on June 3, 2016, the foregoing was filed electronically with the Clerk of the Court to be served by operation of the Court's electronic filing system upon all parties.

/s/ John J. Driscoll